UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

v. 23 CV 9518 (PAE)

SOLARWINDS CORP., et al.,

Oral Argument

Defendants.

----------x

New York, N.Y.
May 15, 2024
2:00 PM

Before:

HON. PAUL A. ENGELMAYER,

District Judge

APPEARANCES

U.S. SECURITIES AND EXCHANGE COMMISSION
BY: CHRISTOPHER BRUCKMANN
BRADLEY NEY
LORY STONE
JOHN TODOR

LATHAM & WATKINS LLP
Attorneys for Defendants
BY: SEAN BERKOWITZ
SERRIN TURNER
KIRSTEN C. LEE
NICOLAS LUONGO

(Case called)

MR. BRUCKMAN: Good afternoon, your Honor. Christopher Bruckmann, for the SEC.

THE COURT: All right. Good afternoon.

MR. TODOR: John Todor, for the SEC.

THE COURT: Good afternoon.

MR. NEY: Brad Ney, for the SEC.

THE COURT: Good afternoon.

MS. STONE: Lory Stone, for the SEC.

THE COURT: Good afternoon.

You may all be seated.

MR. BERKOWITZ: Sean Berkowitz, for SolarWinds and Mr. Brown.

THE COURT: Good afternoon.

MR. TURNER: Serrin Turner here.

THE COURT: Good afternoon.

MS. LEE: Kirsten Lee, for defendant.

THE COURT: Good afternoon.

MR. LUONGO: Nicolas Luongo, for defendant.

THE COURT: Good afternoon.

And good afternoon, as well, to the members of the public who are here today.

Let me begin by just complimenting all of you on genuinely first-rate briefs on both sides. It's a fascinating case, and I have been the beneficiary of really first-rate

lawyering. So I thank you.

I know my law clerk reviewed with you the timing constraints we're under, but I'm chairing a panel this afternoon that requires me to have a hard stop at 4:00 o'clock. We'll take a ten-minute break in between. That means each of you has 55 minutes.

SolarWinds will be going first, and I understand, from my law clerk, that Mr. Berkowitz will go first and then Mr. Turner. And you wish to reserve ten minutes for rebuttal, correct?

MR. BERKOWITZ: Correct, your Honor.

THE COURT: Very good. All right.

So we'll take a break at about 2:45. With that, the floor is yours.

MR. BERKOWITZ: A lot of ink has been spilled, as you know, your Honor. I want to focus on the areas that are of most interest to you.

This is an unusual case in a lot of ways, including that at the motion-to-dismiss stage, it's not just a case that impacts SolarWinds, is incredibly important to SolarWinds, but it also has deep policy implications with respect to your ultimate decision, and that's why you saw the unusual situation for amici filing briefs here. The consequences of a denial of a motion to dismiss, from a policy standpoint, are significant, and we'll talk about those.

THE COURT: May I just ask, without developing it at this point, the claims or the issues that have broader implications are the accounting controls and disclosure controls ones and the response to the SUNBURST attack, but the claims that are earlier in time seem very ordinary. They sound like a lot of cases that this and other courts see in which companies make risk disclosures about products, and then learn that there are some problems with their product.

Why is this any different or have bigger implications than any of those cases?

MR. BERKOWITZ: Yes.

Your Honor, the risk disclosure issue, in particular of the two issues that relate to the prior in time, does have significant implications.

Alleging that a risk factor is -- subjects somebody to liability is actually an unusual issue, to begin with. Typically, risk factors, as your Honor knows, are used in bespeaks-caution cases as a shield against affirmative positive statements that are elsewhere. Here, it's being used as a sword, as a standalone liability for disclosing a risk and not disclosing more.

There are only limited circumstances — the *FBR* case talks about this — only limited circumstances in the Second Circuit that have ever allowed a risk factor to be used as a standalone 10b-5 false statement, and those situations arise

where the risk that is being warned against, such as in the *Meyer* case or the *BDM* case, has already occurred, right? We are warning you against the fact that we could violate laws and regulations, but, in fact, we're already violating them. That's one instance where it has been found.

The other instance — and it's somewhat related — is when you make a positive correlative statement within the risk factors that is made misleading in some way by omission. Neither of those is the situation here. In this situation, your Honor, the only two cases that deal directly with -- in other words, the third issue is, there's no pure omission liability. Here, like *Macquarie* and others, you don't have an independent duty to disclose these issues. And so the only cases that are on point are the *Equifax* and *Qudian* cases, and in those cases, the court found that the risk factors, as they stood alone, were not misleading.

THE COURT: Well, there comes a point at which Government Agency 1, or A, and Cybersecurity Firm B, putting aside what happens later, report malware in what amounts to as pled the company's chief product, this Orion software product, which is said to be the 45 percent source of its revenues. The question is really whether the boilerplate or generic risk disclosure is up to the challenge of capturing that once the company knows that its chief product had two separate customers — private sector, public sector — reporting malware

in it, perhaps under circumstances under which it's fair to generalize that that infects other customers' product, why is the risk disclosure not terribly out of date at that point?

MR. BERKOWITZ: At that point, your Honor, both -- so you have the DOJ, which occurs in May, as reported to the company in June, and then you have the PAN, Palo Alto Networks, which is reported to the client in October. Neither of those issues -- and if you look at paragraphs 270 and 284 of the complaint, amended complaint, the company does not make any conclusions about the source of that attack. And this is all within the four corners of the amended complaint. The DOJ incident, your Honor, was an incident where they said we're not sure what we have, and the company never determined what it was. It very well could have been, at the time, software or an invasion on DOJ's network that somehow it infected or was related to the SolarWinds' software.

Similarly, in October, at paragraph 284, there's no conclusion that that incident was related to a specific issue on SolarWinds' software as opposed to the customer software.

THE COURT: Wasn't there chatter within relevant players in SolarWinds connecting the two incidents?

MR. BERKOWITZ: Say that again?

THE COURT: Wasn't there discussion within your client's company connecting the two incidents, tending to suggest that this was not an artifact of some problem just

within DOJ or a problem within PAN as opposed to something that was a problem within the product?

MR. BERKOWITZ: There was discussion about whether it was related, for sure, but the discussion did not arrive at a conclusion, and there was never a conclusion that, in fact, the -- that the incidents were related or that they were related to a software infection.

According to the complaint, both DOJ and PAN reported that somehow there was information that was being sent out of the -- you know, related to the software, perhaps appearing to be communicating or sending out information related to SolarWinds, but there was no specific conclusion. And if, at the end of the day, what we're talking about is a scenario or situation when you've got incidents to which there's no conclusion, SolarWinds would have to report that, it would create mass confusion. There are customer incidents all the time. Microsoft gets customer incidents all the time. And where there is no specific conclusion or determination, it would create havoc to say, hey, we may have something, we have no idea exactly what it is, we have no idea how to fix it.

Looking at the statement, in fact, those are consistent with the fact that we are vulnerable to attack, and that's what we are ultimately talking about, is whether the risk factor itself is misleading.

This is a company that, as soon as it learned that it

had software that had malware on its software, that it was sending out through updates, reported it within two days. There is no evidence in the record that suggests that that determination or anything close to it was done.

THE COURT: May I ask you this: One of the questions in the case involves the interplay between — and I'm stopping the clock right now before SUNBURST --

MR. BERKOWITZ: Yes.

THE COURT: -- the interplay between the risk factor disclosure in the relevant SEC filing and the security statement, which is a big focus of the SEC's complaint, and the thrust of which is that it blows sunshine over a bunch of genuine security problems that is alleged to come home to roost. Are those really segregable? In other words, can the problems alleged in the security statement be considered in considering, I guess it's, claims 5 and 6, which relate to the filings?

MR. BERKOWITZ: They absolutely are segregable, your Honor. This is not a situation where the customer-facing security statement that Mr. Turner will talk about, which is on the website under various clicks when you ultimately get to it, was adopted or incorporated by reference.

I think it may be helpful — and we cited the *Marsh & McLennan* case — to say you've got to look at the statement in the context in which it's made, but let's pull up the risk

factor disclosure, your Honor. Again, this is a robust disclosure about the various concerns that are raised, talking about systems being vulnerable and so forth, and it goes into detail both at the general and specific, including sophisticated named state attacks and so forth. The final bullet, and these were excerpts from risk factor, says, "Despite our security measures, unauthorized access or security breaches could result." This is not like in the *Fannie Mae* case, where they brag about how robust their risk compliance is. This is a situation where they say, look, despite our security measures, unstated, unlinked to, unreferenced to a security statement that dates back to pre-IPO, we are at risk of all of these serious things happening.

So it's not fair to incorporate them by reference. In fact, the question is, is this statement misleading as it stands, is this risk factor, which is warning of the exact risk that materialized, inaccurate?

And the SEC doesn't really point to those two prior issues. Basically, what they say, when asked, is, well, there should have been either more adverbs like heightened risk of your critical assets, or you should have disclosed that you had access control problems.

THE COURT: Just a hypothetical: At what point would a series of customer reports about malware being found and a common problem give rise to a viable claim that the risk

disclosure is too generic, that it's not up to the task of capturing what the company then appreciates?

MR. BERKOWITZ: I would say when the company makes a conclusion that it has been hacked, your Honor.

THE COURT: And you're saying that the pleadings from the SEC pre-SUNBURST don't get there?

MR. BERKOWITZ: Yeah, they do not. The only principle that you can look to, ultimately, when you're in the room trying to figure out, okay, does this rise to the level of being reportable, the only thing that you can do, the only right line that's out there is materiality at the end of the day. What I can tell you is that the two customer reports here are so far from the materiality line, particularly given the specific allegations of the complaint, that there was no determination made as to what the source, ultimately, of it was.

THE COURT: But had the company concluded, stitching together reports it had gotten from multiple customers, that these separate events must bespeak an attack that got in at the SolarWinds level and not at the customer level, would that change the outcome?

MR. BERKOWITZ: Again, it comes back to materiality, how big, what the exposure is, and those types of questions, I would say, your Honor. Regulation S-K obviously says you've got to disclose the material risk if, in fact, you are not just

vulnerable, but you believe that that vulnerability has actually occurred because of these various customer incidents, then you would have an obligation to update it.

Here, there are no allegations that that occurred.

And what's really dangerous about this, and why we sort of got off on this tangent as a critical issue, is you asked whether this isn't just a garden-variety issue. What you're talking about here, right, is a determination that there is a materiality obligation to disclose risks or incidents as they're coming in. You've got almost like a TikTok update requirement of people saying, well, what about this, where do we go, what about this particular risk issue, is that something that we think is a particular concern or an area? It's dangerous to go down what is a slippery slope of saying one report, two reports; you really have to draw a conclusion that --

THE COURT: One thing that's a little different about this case, though, is that it's not a generic cybersecurity risk that any company in America that sells pizza or TVs or cars might have. This is a cybersecurity risk involving a company that sells cybersecurity, that sells software, and the issue here is not do you have to disclose incremental problems with your alarm system, it's at what point do we have to disclose the fact that our flagship product might be corrupted.

MR. BERKOWITZ: Well, look if we're away from having

disclosed -- to disclose problems in our cybersecurity measures, and we're only focused on when you have that obligation, your Honor, I think that's a different case than what the SEC is suggesting. That's more narrow.

But keep in mind, what you just said, this disclosure, right, is not a generic restaurant disclosure. The first line is, "We're heavily dependent on our technology infrastructure," right? Our systems are vulnerable to hackers and malicious code. It's leading with that issue, right? This is a risk disclosure that is specific to this company and the risks that it faces.

And I think when we talk a little bit more when we get to the 8-K, because there's a similar issue, shouldn't you have disclosed those two incidents — we can get into a little more detail about those two — but I think if we're really just talking about those two, the fact that the company did not make any conclusion about the source of those ought to be dispositive from a materiality standpoint.

THE COURT: When does the company as pled draw that conclusion?

MR. BERKOWITZ: When did the company?

THE COURT: Yes. Is it after SUNBURST, in effect after December 12th?

MR. BERKOWITZ: In December, Mr. Brown — December 13th, I believe — and there's testimony, I think it's

in paragraph 308, it's in that range — says, once I actually saw the uncompiled source code -- so what you had happen, right, I think it was Mandiant/FireEye was the customer who reported, hey, your updates have this malware. And they actually provided a copy of the malware. And what that malware showed was something that, to Mr. Brown, said, hey, this malware is sending the same -- it looks like it's consistent with what customer A and B had reported, that they were linked.

So, remember, when we were here last fall, I guess, the SEC said, the fraud ends in January, when the company makes its disclosure. And all they disclosed in January — and it's Exhibit 4 of our brief, and I'd urge you to look at it — is that with the benefit of hindsight, the company concluded that these customer incidents were linked to SUNBURST, not that they were something that revealed anything much more meaningful than that.

So, in December, there is a conclusion in Mr. Brown's mind, and by January, the company reports it, but it was not done before that.

So let me pivot, if I may, to scienter on this because our discussion on this, on what's material and how difficult it may be to grapple with that, it's stunning because you would think that in a case charging 10b-5 and 17a-1, you would have a situation where they said the maker of this statement knew that it was wrong, that this risk disclosure was wrong, right? The

only people who signed this are the CFO and CEO of the company, and there is not any allegation that either of them acted with intent. Instead, the SEC has charged, at the time, the vice president of security and architecture, later the CISO, Tim Brown, was remarkable about the fact that he is the individual who was supposedly acting with intent, is that he never saw this risk factor we're looking at now.

THE COURT: He never saw it or he never signed off on it before it issued?

MR. BERKOWITZ: He never saw it. Paragraph 242 is the specific allegation, and they concede he testified, he did not review the precise disclosure language they use.

Mr. Brown is not a disclosure expert. He wasn't even an officer of the company at the time. He was the chief security and architecture.

THE COURT: And do you understand, though, that the SEC to be claiming that as to scienter on, I guess we're talking here about, claim 5, right — that's the false filing claim — that the scienter is anchored just in Mr. Brown's state of mind?

MR. BERKOWITZ: Yes. I mean, they hinted at the potential for some collective -- almost a throw-away, some collective scienter, right, the *Teamsters-Dynex* case that cites *Tellabs*, that if they say we've made a million trucks, and they really haven't done any, somebody must have known, but

Mr. Brown is who they're relying on for their scienter here. He never saw it.

All they allege is that he provided information to people who ultimately did the risk factors. They don't say what he provided, when he provided it, or that he was intending to withhold it. And keep in mind that under *Seltzer*, right, when you're looking at intent, there has to be a clear duty to disclose, right? A clear duty is not in existence here. We're debating, and we spilled a lot of paper on this. And then you have to prove that he acted with a requisite level of intent as to the risk disclosure, right?

They failed at the start that he didn't even know the specific statement that was made. But even if they did, he has to act with either knowledge or recklessness. And recklessness here, as your Honor knows, is acting essentially with actual -- is something approaching actual intent or an extreme departure.

THE COURT: According to the pleadings, when did the CEO and the CFO, who were responsible for the risk disclosure, become aware of the earlier two cyberattacks by customers A and B?

MR. BERKOWITZ: I think that the -- I don't think the record is clear on that, your Honor. I think the -- I believe that the disclosure that's made is in January. But Mr. Brown, there's no allegation that he was intentionally withholding it. There is a disclosure issue where they say there's an incident

response plan. One of the disclosure controls that's in place is an incident response plan, where the company is supposed to grade on 0 to 3 or 4. And Mr. Brown grades both of these as 0, meaning that the source of it is unknown, which is what they concluded and what is in there. And there's no allegation that he did make that conclusion or that he was intentionally withholding the information, nor would it make any sense.

There are a number of allegations — paragraph 121, 192, 167 — of Mr. Brown providing updates to the CIO, chief information officer, chief technology officer, that make their way to whatever. There's not any allegation that there was an intentional effort to hide this information so that it wouldn't be disclosed to the public.

THE COURT: While we're on that, let's just take a detour. I understand you're the right person to ask about the disclosure controls claim. Since we're dancing around it, let's just address that right now, if I may.

MR. BERKOWITZ: Yes.

THE COURT: The argument anyway, but the allegation is that the information of the heightened risk, however it's characterized, didn't essentially reach the C-Suite, that the control environment should have resulted in at least had the potential to be a grave risk directed to a flagship product should have hit the C-Suite and didn't.

MR. BERKOWITZ: Correct, that's the allegation.

THE COURT: Right.

MR. BERKOWITZ: The simple answer is that there were controls in place that were designed to raise to the level of the people in charge of disclosures if --

THE COURT: Sorry, but on the pleadings, where I have to take the facts that are well pled as accurate, that sounds like a factual dispute, whether or not there were adequate controls in place.

MR. BERKOWITZ: I, respectfully, disagree, your Honor. I don't believe the SEC is suggesting the controls were inadequate. What they are saying is they weren't effective and they weren't executed properly.

THE COURT: They're saying the proof is in the pudding, that while you can't always back out of a bad disclosure controls environment from the failure on a particular occasion, they're basically saying, hey, look it happened twice and didn't reach the C-Suite, and, ultimately, of course, it turns out to be an epic problem.

MR. BERKOWITZ: Yes, but that, again, is an execution issue, that is not a design issue. The design was there. What they're saying is they have should have raised it a 2 or a 3.

THE COURT: Right, they're saying that Mr. Brown, they say, deliberately, but be that as it may, errantly miscast this as a nothing burger where it was a something else that should have been elevated, and because it happened twice and involved

the flagship product, they infer from that, that the disclosure environment was not up to the task. That's the thrust of it, right?

MR. BERKOWITZ: I think you've perhaps even articulated their theory better than they did in the papers, but what I would say is it still comes down -- this is two incidents. It's not a situation where we've got dozens of incidents. It's two incidents, both of which, in the complaint itself, are alleged that they couldn't determine. And, by the way, it's not -- it's not unusual that they didn't. If you look at page 7 and on the CISO briefs, right, they tell you how sophisticated this attack was. I don't want to understate that. And it's a good pivot, perhaps, to the 8-K, as Mr. Turner reminds me --

THE COURT: Let's get to that, but the one question is: Both customers seem to treat this as a very big deal when they report it to the company; they're not treating it as something minor, right? Doesn't the customer's labeling of it matter?

MR. BERKOWITZ: Nobody was treating it as a small deal. In fact, in this environment, everybody works together to try and figure out what happened.

DOJ, the allegations are, they worked with two security firms to try and understand what was happening. Nobody concluded that the malware was inserted at SolarWinds,

and it was put out. Nobody made that conclusion, neither PAN, nor DOJ. So it wasn't as if they said, hey, guys, you have malware on your software. That absolutely was never disclosed, and they themselves didn't draw that conclusion. They're saying, hey, do you know what this is, is there anything that we can come up with?

And so this is an incredibly difficult to figure out situation. Ultimately, it's figured out. Maybe if we look at what we're talking about.

If we can look at 4, and I will -- let's actually look at the -- one more, yes.

This is an exhibit in the brief that's cited there, your Honor. The first three pieces of this --

THE COURT: Sorry, just so we have a record, this is the exhibit cited at defendants' brief at 5 and 18.

Go ahead.

MR. BERKOWITZ: Correct.

So the first three steps here, to be really clear, are the Russian state actor implanting in SolarWinds the malware. And they actually inserted it in a way after it was production ready right before it's shipped out. That's where it was inserted.

It then gets sent between March and June via hotspot updates to up to 18,000 customers who downloaded it, could have installed it, et cetera. So what we're talking about here is

that those two customers, Mr. Brown ultimately linked them saying, hey, they have this software. Nobody concluded steps 1 through 3 at the stages of either the DOJ or the PAN incident.

THE COURT: He drew a connection between the two, but didn't you say drew a conclusion as to how they got there?

MR. BERKOWITZ: Certainly not by those time periods. That's absolutely right, your Honor.

THE COURT: Before you move just to the 8-K, just one final question on this point: I take the defense's position to be that the accounting control rules simply don't apply to this situation, and that the disclosure rules, in theory, could, but factually, are not -- it's ill pled?

MR. BERKOWITZ: Correct, yes.

So, again, 4 and 5, to be clear, that's a backdoor. The malware that's inserted on SolarWinds' software that gets updated is a backdoor that, when running and connected to the internet, allows the threat actor to potentially try and get in the backdoor. That's number 6 and 7. That's the infiltration, right? 4 and 5 were on the server. 6 and 7 is using that backdoor, opening the door, and walking in to the customer network, which is where all the valuable information ultimately is.

THE COURT: That ultimately happens to customer C, but not as pled to A or B?

MR. BERKOWITZ: There's actually no evidence in the

record that anybody was infiltrated, your Honor, and we'll talk about that real quickly.

So let's get to 2, which is the 8-K disclosure. I want to make just a couple of key points on this.

So this is the 8-K disclosure. When this was disclosed, this dropped within a couple of days 25 percent, okay? Big deal disclosure.

Made aware of the cyberattack that inserted a vulnerability. That is the backdoor within its Orion monitoring products which, if present, meaning if it was actually downloaded and installed and activated, could potentially, if it was connected to the internet, allow an attacker to compromise the server. Likely the result of a highly sophisticated target attack. This was inserted in products from March to June and up to, SolarWinds currently believes — this is the fourth bullet — that the actual number of customers that may have had an installment of the products containing the malware to be fewer than 18,000. In other words, up to 18,000 had this malware on their system.

And the fifth bullet says there have been significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing the attack to a vulnerability. And so this is a huge deal. And what the SEC is saying is, you should have disclosed that of those 18,000 customers, you actually knew who two of them were.

THE COURT: I think what they're saying is a little bit different. They're seizing on the word potentially in the first bullet. They're saying that the word potentially smudges the fact that something actual had happened.

MR. BERKOWITZ: And I think that's not a factual issue, your Honor. What they're saying is — and I believe it's in 258, paragraph 258 — if this software, right, it's downloaded by up to 18,000 customers, but those customers not only have to download it, they have to install it, they have to be running it, and it has to be connected to the internet. A lot of these companies have closed loop servers. And they also have situations where they have their own firewalls in place.

So this is an absolutely accurate and fair statement, could potentially allow an attacker, right? They allege --

THE COURT: Sorry, but as to company C, did the facts go beyond "potentially"?

MR. BERKOWITZ: I don't -- it went beyond -- it did in the sense that they were aware of the attack. So I believe it went beyond that because they downloaded it.

THE COURT: Look, with company C, doesn't company C basically say, yes, as to activated?

MR. BERKOWITZ: No. I mean, there was no breach of company C. All they did was call and say, hey, this is out there. They did not say -- but the "potentially" here is saying that -- I want to really stress the significance,

your Honor. This is not a, hey, it might be a problem. This is, there's a huge problem.

THE COURT: No, no, no. Look, the truth is in the reaction. The stock drops a lot. It's a big-deal disclosure. The SEC's argument is it doesn't go as far as what the company knew, and what they're basically saying is it's a little bit like saying tainted Tylenol, it could kill somebody when it, in fact, already has.

MR. BERKOWITZ: Again, what they're saying is that up to 18,000 customers downloaded this malware, and it could potentially be exploited. It wasn't exploited or infiltrated, it absolutely was not with respect to customer C, and there's no allegation of it.

Take a look at the fourth bullet what's going on -- I'm sorry, the third bullet. SolarWinds has retained third-party experts to assist, including whether the vulnerability, meaning the downloaded malware in the products, was exploited as a point of infiltration. That's the key issue for people — did they access the networks, your Honor? Did they access the networks?

And there is no evidence — the record is bereft of any evidence — that anybody had been exploited. That was on that chart, 6 and 7. The backdoor existed. The question is whether people went through it.

THE COURT: So just factually, what is it that

company C, as pled, tells SolarWinds on December 12th about what, in fact, had happened to it?

MR. BERKOWITZ: That there was a cyberattack -- that there was the presence of this code on SolarWinds' software. That's all.

THE COURT: Not that it had reached the server of company C?

MR. BERKOWITZ: Correct.

THE COURT: Go back to the "potentially" language, please, on the slide.

So potentially modifies allowing the attack to compromise the server. I think what you are saying to me is, while potentially might have been a problem with it modified something else, it's not a problem with the clause that it modifies because, in fact, the attacker, at least as revealed at that point to SolarWinds, hadn't compromised the company C server. Is that accurate?

MR. BERKOWITZ: Correct.

And I want to -- in our briefs, there were probably particular hits on this. I want to touch very briefly on this because Mr. Brown did review the 8-K for technical accuracy, but, again, he's not a disclosure expert, and the concept then, looking at this statement, which is incredibly detailed, that he should have made the conclusion that there was a clear duty to talk about these two other issues or -- and, again, the

third issue was known to everybody, and none of them were alleged to have done something wrong. So the issue really is those two prior folks. That he should have had knowledge of that is just absolutely -- there is no imputation. He's the one that they're trying to impute this issue to, your Honor. And, in fact, when it's ultimately disclosed that these two customer incidents were, quote, linked --

THE COURT: Which is in January?

MR. BERKOWITZ: Yeah.

-- nothing happens to the stock price. That's not dispositive, but that gives you a sense of how small a deal that issue was. And it was in the context of the company updating, in detail — and I urge you to look at that — in detail what the results of their investigation were. And they hadn't concluded by that time or at any time, relevant to this complaint, that anybody had actually been infiltrated, meaning that it had gone to the customer network, which is where all the goods are.

So, your Honor, with that, I'm going to -- I'm happy to answer other questions --

THE COURT: No, let me hear from Mr. Turner on what happened to the preceding claims involving the security statement, and I understand that's what you've allocated to him?

MR. BERKOWITZ: Correct.

THE COURT: Okay. Thank you.

MR. TURNER: Good afternoon, your Honor.

THE COURT: Good afternoon.

MR. TURNER: So the SEC's claim is based on the security statement. They rest, basically, on five assertions in that statement. And I'd --

THE COURT: Before you get to the individual ones, your colleague, Mr. Berkowitz, made a point of saying that it's customer-focused, it's on the website.

MR. TURNER: Yes.

THE COURT: You're not arguing, though, that that makes it, in some sense, incapable of being actionable as the basis of a 10b-5, are you?

MR. TURNER: Not incapable. It makes their scienter less plausible.

THE COURT: Why is that?

MR. TURNER: Because if the company actually had some intentional plot to deceive investors about the security, you would think they would say something affirmative about their security in their investor disclosures, your Honor. The investor disclosures said nothing affirmative about the company's cybersecurity.

And just to come back to that point, the key question for the risk disclosures is whether they were misleading. It's not whether they were generic, it's whether they were

misleading. The risk disclosure clearly disclosed the company was vulnerable. That was not misleading.

The issue of whether it's generic enough just goes to whether it can be used for bespeaks-caution purposes.

THE COURT: Right, I understand that. But the SEC makes a detailed set of allegations impugning the accuracy of the security statement. I know you're about to get into that in detail, but if you assume, just for the purpose of this moment in the argument, that the SEC has something there, and that what is said in the security statement is impeached by what was internally known, is there a reason why that couldn't be the basis of a 10b-5?

MR. TURNER: In terms of imputing Mr. Brown's intent, no, that does not work.

THE COURT: Well, he has said to have known not X when the security statement says X.

MR. TURNER: Right. So that's the security statement, but if we're talking about the risk disclosure, the important intent that needs to be imputed is knowledge that the statement in the risk disclosure is false.

THE COURT: Wait, sorry. Suppose the SEC had not brought a claim based on the risk disclosure, but simply brought a 10b-5 claim based on other statements, including in the security statement. Why would the risk disclosure matter?

MR. TURNER: Right. So if we're putting aside the

risk disclosure, and just talking about the security statement --

THE COURT: That's what I'm asking you about.

MR. TURNER: Yes.

I just mean in terms of if the allegation is that there was an intentional scheme to mislead investors, this is a particularly odd way to do it.

THE COURT: Through the customers?

MR. TURNER: Yes.

THE COURT: But, look, it's on the website, it's on the website in apparently a way that's able to reach your garden variety customer. Why can't it do double duty and also reach an investor?

MR. TURNER: Your Honor, I'm not saying it's impossible, I'm not saying legally it's completely wrong. I'm just saying if there really were an intentional scheme to mislead investors, the clearest way to do that would be to speak to investors and make claims to investors about the quality of the cybersecurity code. That isn't done in the risk disclosure. The customer-facing security statement was customer-facing.

THE COURT: Is there a case law that draws the line you are drawing that, in effect, diminishes the probative value, if you will, in a fraud case of the statements made to customers?

MR. TURNER: There is one case, your Honor, the *Allscripts* case, it's a Northern District of Illinois case, and it just notes that in that case, the statements were particularly immaterial given that they were in a venue directed towards customers rather than shareholders. I really don't want to get hung up on this issue because we're obviously not making our -- our main argument is not that it's customer-facing, therefore there could be no fraud. And the SEC has really walked away from their intentional scheme allegations. They're really resting on just a recklessness or knowledge theory. But there are a number of reasons why the idea that Mr. Brown was engaging in an intentional scheme is absurd to begin it, but I do want to make sure to get to the actual substance of the security statement, your Honor --

THE COURT: Go ahead.

MR. TURNER: -- if you'll permit.

THE COURT: Yes, go ahead.

MR. TURNER: So, as I mentioned, there are five areas where they focus on in the security statement. But just to focus for a minute on the SEC's pleading burden here, these are statements of policy. That's what they're challenging. These are what the company works to achieve. These would never be reasonably construed as guarantees of perfection. The case law recognizes that, and the SEC recognizes that.

They keep repeating in their complaint, these are not

isolated problems they're alleging, they're pervasive failures, longstanding pervasive failures, et cetera, et cetera. They cannot just mouth those words. That is not something that can be alleged in a conclusory fashion. Under Rule 9b, they have to allege particular facts to show pervasive allegations.

They try to bluster their way past that pleading burden with a large number of allegations, but they do not get points for work count here. They have to plead specific facts showing how and why each of these statements in the security statement is false, and they fail to do so.

THE COURT: Well, look, the access controls, for example, there are some pretty detailed allegations that the company was touting the access controls as muscular whereas, in fact, they were porous. That's basically put in Mr. Brown's mouth.

MR. TURNER: I can jump to that one, your Honor. I was going to go through one by one.

THE COURT: You're welcome to. I want to make sure you use your remaining time wisely, but there do appear to be substantial allegations that Mr. Brown was on notice as to the inaccuracy, at least, of some of these.

MR. TURNER: His statements are not alleged to be -- adequately alleged to be inaccurate in the first place. I can argue that. I can get to the access controls issue. These are the problems with the allegations, however, your Honor, just to

separate them out real quick, because it is important to separate them out. Even if the Court finds one or two of these salvageable, it's very important to weed them out. If they are not salvageable, that is the other gatekeeping rule of 9b here — to the extent the case goes forward at all, there's a lot of work that can be done to narrow the scope of the discovery and litigation.

But just to start with NIST, your Honor, so they have this allegation that the company says it follows the NIST framework. We've explained in our brief that -- and as the SEC itself acknowledges, the NIST framework is a self-evaluation framework. That's clearly articulated in the NIST guide --

THE COURT: Your point is that this 800-53, that point is just simply not pled?

MR. TURNER: Your Honor, if you want to look it up, it's on the internet, but 800-53 is just like an informative reference that you can use. It specifically said when you use it that way, it's not like a checklist.

THE COURT: That's why I went to the access. I was not seizing on that one.

MR. TURNER: Yes. I can skip back to the NIST statement, if your Honor is already convinced on that point?

THE COURT: Well, I'm not stipulating to that, but I do agree that within the range of the allegations, this is not their strongest one.

MR. TURNER: The key point is you're using it as a self-evaluation framework. It's fundamentally what it is. It's a statement about process, not substance, that you have a process for evaluating your cybersecurity in these areas, and you constantly evaluate yourself in using the framework.

But I think the SDL is also important to look at, your Honor.

This is an important way in which the allegations don't meet their pleading burden. So they allege that SolarWinds pervasively failed to follow an SDL, a software development lifecycle. That is directly contradicted by documents the SEC cites in its own complaint. So if you look at what it describes as an audit in April 2018, even by that early point, this document clearly states that the company had implemented the SDL.

THE COURT: I think paragraph 122, though, has contrary allegations from December 2018, which is later, in which the presentation says, "We have no formalized testing with respect to" --

MR. TURNER: That's pen testing. First of all, they say they didn't implement the SDL. This says they did implement the SDL. Then you get the pen testing, right? And so, again, you have a document that says from August 2019, this is the NIST scorecards again that they repeatedly cite and credit. It says, very clearly, the company had a program for

penetration testing in place, they gave itself a 4. When you look at what they are citing, your Honor — I'll jump to that — they're citing things like -- here's what they cite: One line in a presentation that says that a particular pen testing project was unfunded. That doesn't mean there was a pervasive failure to implement a program. All it means is there was some sort of line item that was unfunded.

If you look at other things they cite, this is from October 2018, it indicates there was pen testing going on at that time — pen testing complete for MSP products. This is external pen testing, bringing in somebody external to do the pen testing. Pen testing is good for Cloud products, not for the Orion products, because there was an internal team staffed for that.

So it's very important, your Honor, to look -- this is not a case where the SEC has any witness who ever told them that SolarWinds pervasively failed to do anything. They had three years to investigate. They didn't give one witness. All they are doing is picking out -- cherrypicking snippets of documents and trying to pass them off as pervasive failures. And if you look at the documents we have put before the Court, which are documents they cite, the allegations are contradicted by those documents, and if you look at the counter-- the pieces of evidence they're citing, they're making unreasonable inferences from those documents.

And this is not a factual dispute, your Honor. We're not seeking to introduce our own evidence here to challenge the SEC's allegations. If you --

THE COURT: Go to access controls, because it seems to me that there's a different quality of the allegations there. The representation in the security statement is that the access controls are role-based and that the access controls to sensitive data are set on a need-to-know least-privileged necessary basis, and the SEC pleads facts that administrators or employees were given unnecessary administrative rights that most employees had. I think there's an allegation that the password was something like 123.

What's the problem with that pleading?

MR. TURNER: Well, passwords and access controls are two different issues they treat. But passwords, that's a -- that's an example right there of the cherrypicking that's going on. That is one password on a single external server the company was using for a particular purpose. That does not imply that there is a pervasive failure to implement a password program. All the time -- what a cybersecurity program does is find gaps and remediate them. That is the everyday functioning of a cybersecurity program.

So when the company finds some system that it has an errant password on and fixes it, that doesn't mean there's a pervasive failure. That is the company implementing and

maintaining its password policy, fixing that issue. If you look at -- we cite, your Honor, these -- I'll throw it up on the screen for you. Here are a number of cases we cite where courts have found failures to adequately allege pervasive problems. *Hill v. Gozani* is a particularly informative one. In that case, there were allegations about problems with insurance reimbursements, pervasive problems, and the court said -- you know, the plaintiffs filed a 70-page opinion, but when you look at the actual allegations, it's just a smattering of sort of random situations where there were some sort of reimbursement issues. That does not amount to pervasive problems.

These are other cases found similarly. That's what we're asking your Honor to do here. Look closely at the specific allegations being made look closely at the documents they're relying on they don't add up to pervasive problems.

Access controls is no different in that regard.

So they cite the access controls statement. And then what do they show as their evidence?

THE COURT: So August 2019, Mr. Brown prepares a presentation that says, "Access and privilege to critical system/data is inappropriate."

MR. TURNER: Correct.

THE COURT: Why isn't that an admission that, on the pleadings, can be taken as fairly pleading pervasiveness? This

is the chief guy in this area saying something very declarative like that.

MR. TURNER: Something, but it's unclear what that something is. What exactly is inappropriate?

Access controls, there can be a wide variety of issues affecting access controls. For example, what the SEC was actually told in depositions in this case — this is obviously outside the record, but just to provide an --

MR. BRUCKMAN: Objection.

THE COURT: Overruled.

MR. TURNER: -- example — is when employees were onboarded or offboarded, the processes were manual in place instead of automated, and that can be unreliable. And so the company was interested in maturing those controls to make them automated. It has nothing to do with least privilege, and it has nothing to do with a pervasive failure to have access controls.

THE COURT: May I ask you, just connecting up to what later happens, do the pleadings trace what ultimately winds up being the SUNBURST attack to a security weakness within the company?

MR. TURNER: No, your Honor. And that's really -- all they say, for example -- all they say about the security development lifecycle, for example, and the failure to implement controls of the product quality, completely

irrelevant. The attack that happened here was not an exploitation of some existing vulnerability in SolarWinds' product. It was the Russians coming in and implanting their own vulnerability. It was not some sort of sloppiness in the way it was coded.

THE COURT: You're saying the complaint does not allege that the Russians exploited some deficiency for which SolarWinds was accountable?

MR. TURNER: The only connection they try to make is that they say that the attacker used the company's VPN. There's nothing said in the security statement about the VPN in the first place.

But the SUNBURST attack is being used as an excuse to bring this case. It's not really what the case is fundamentally about, especially when it comes to the security statement.

THE COURT: Mr. Turner, you've got several more minutes. I want you to hit the most important points.

MR. TURNER: That's the important thing, your Honor.

The Second Circuit has stressed, Rule 9b requires them to allege exactly how and why whatever allegations they're relying on show that the statement made was false. And just pointing to a one doesn't necessarily mean that these statements, these specific statements, the access controls sections were false. They had three years to investigate.

They had three years to figure out what exactly that one means and explain it to the Court. So they can't just rely on that conclusory or just sort of a vague allegation without tying it specifically to the statement in the security statement.

But, your Honor, I would just say, if you're not convinced, and access controls, you think there's been enough pled to let it go forward, let the case be just about that. There's so much narrowing so we can -- that is an issue that we could have discovery on, finish up, and brief summary judgment in 60 days.

THE COURT: So let me ask you a final question, which really picks up with the very first sentence of Mr. Berkowitz's argument. If the case reduced to the security statement as the basis for a 10b-5 claim, to what degree does this implicate the broad policy issues that Mr. Berkowitz is concerned about?

MR. TURNER: I think if your Honor were to get rid of the risk disclosure piece and get rid of the 8-K piece, and all we're talking about is the security statement and pieces of it, that would resolve many of the policy concerns at issue.

THE COURT: At that point, it's an as-applied facts and circumstances issue, and the issue before me is has the SEC pled enough consistent with 9b to get to discovery.

MR. TURNER: Yes. And then we're not talking about -- we talked so much in the risk disclosures discussion about those two prior incidents, and that's not really the focus of

their risk disclosure claim. They're risk disclosure claim is, companies should be disclosing a lot of details about their cybersecurity programs and what's wrong with them in their risk disclosures. That's what amici are worried about, that's what industry is worried about, because they are left in the lurch, what are we supposed to disclose, there's no limiting principle, there's no articulable principle here, and, all of a sudden, we're being told that we have to disclose all sorts of things that can be valuable to hackers.

THE COURT: All right. Very helpful and very helpful context.

Let me ask you this: You've got a PowerPoint that you've drawn upon to something, but not merely as much as you intended. Can you please file a copy of it on the docket of the case? I'm going to mark it as Court Exhibit A. It's important that I make a record of what was before me during the hearing.

MR. TURNER: Of course, your Honor.

THE COURT: We'll take a ten-minute comfort break, and when we resume, I'll hear from the SEC. Thank you.

(Recess)

THE COURT: All right. I'll hear now from the SEC, and Mr. Bruckmann, I gather you're going first?

MR. BRUCKMANN: Yes, your Honor. And with the Court's permission, I'll argue from the table, if that's all right.

THE COURT: That's fine, just as long as you speak into the mic.

MR. BRUCKMANN: May it please the Court, Christopher Bruckmann, for the SEC.

Material statements by public companies and their leaders have to be truthful. They have to convey the whole truth. And that is the case, and has long been the case, regardless of the topic, whether it's a product under development, security procedures that they're taking, production figures. Once a company speaks on a topic, it has the obligation to tell the whole truth.

The defendants' core position here in seeking to dismiss this entire case is that cybersecurity is the lone exception to that longstanding rule.

They would have this Court find that because telling the truth on cybersecurity can have consequences on cybersecurity and cybersecurity alone, companies must be permitted to lie. No. That cannot be the case.

This case is not just about the SUNBURST attack. The defendants violated the federal securities laws from the moment of SolarWinds' IPO, well before the SUNBURST hack. They did that through material false statements and omissions regarding the cybersecurity practices. The security statement, with specific affirmative representations as to actual practices that SolarWinds was presently undertaking, was false throughout

the relevant time period.

THE COURT: So let's start with that, just because that's where Mr. Turner left off, and his contention is that the SEC is effectively nitpicking and taking statements out of context and that the pervasive security failures that the SEC is pleading aren't backed up by the incorporated documents.

MR. BRUCKMANN: Well, your Honor, let's look at some of the incorporated documents.

If you look at Defendants' Exhibit 7, on the page entitled "Protect" --

THE COURT: Do you have a PowerPoint, or should I be looking at --

MR. BRUCKMANN: I'm old-fashioned, your Honor, if your Honor doesn't mind paper.

THE COURT: I've got the complaint handy.

MR. BRUCKMANN: Well, I can simply describe it, your Honor.

In Defense Exhibit 7, on the page entitled "Protect," in August of 2019, SolarWinds assessed that for the security category authentication, authorization, and identity management, they had a NIST level of 1. And they said that user identity, authentication, and authorization are in place and actively monitored across the country. The score of 1, according to that same document, means that the organization has an *ad hoc*, inconsistent, or reactive approach to the

security control objectives.

And as we explained in the complaint, that is generally considered to be a poor score. That is one of the same documents that also says, "Access and privilege to critical systems data is inappropriate."

Your Honor, I have an extra copy.

THE COURT: I've got it in the version of the -- no, here it is, I've got it. I've got it as an attachment to Mr. Turner's affidavit.

MR. BRUCKMANN: Yes, that's the document I'm talking about, your Honor.

Looking at the complaint itself, if you look at paragraph 194, your Honor, there is a chart. And this is from one of the NIST 800-53 evaluations referenced in the complaint. Regardless of why the NIST 800-53 evaluations were done, they revealed specific information to Mr. Brown and others. And one of them was — and this is for the organization, not for just a product — it says, "The organization (a) limits privileges to change information system components and system-related information within a production or operational environment." The finding was, "No known privilege limitations." That's the last row of the chart in 194 in the amended complaint.

There are pervasive access control problems, not just an isolated problem --

THE COURT: That's of the five items that

Mr. Turner --

MR. BRUCKMANN: Yes.

THE COURT: -- specified. Access controls is, from your point of view, the strongest for your case?

MR. BRUCKMANN: Yes.

But there's plenty to support the others as well. On the secure development lifecycle, part of a secure development lifecycle is having training, threat modeling, and penetration testing. So while SolarWinds claims that they had established a secure development lifecycle, that same document that we were just looking at, Exhibit 7, rates it as a 2, on the page "Identify."

Well, 2, according to the scoring system in that very document, means the organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented.

THE COURT: But by 2019, it's up to a 3, according to --

MR. BRUCKMANN: It's the 2019 document that I'm looking at, your Honor.

THE COURT: Right. But there's a chart. You've chosen to highlight the score that the company gave itself in 2018 as a 2, but the next year, it gives itself a 3, where, although it's not Mercedes-level adjectives here, it's a perfectly solid set of evaluations.

MR. BRUCKMANN: But, your Honor, if your Honor goes a few pages forward in that same document, there's a specific rating for the secure development lifecycle. So that's on the page — it's misspelled — "Indentify," but I believe it's supposed to be "identify" at the top.

This one, your Honor.

THE COURT: All right, keep going. Yes.

MR. BRUCKMANN: That's where there's a specific rating in 2019 for the secure development lifecycle of a 2. While it means there's something in place, it also means that they do not routinely measure or enforce policy compliance. Then if you look at the specific allegations in the amended complaint in that same time regarding the lack of penetration testing, the lack of security training, the lack of threat modeling, that shows that they did not have what they represented in the security statement.

THE COURT: The document that you have just drawn my attention to has a series of missed maturity level ratings --

MR. BRUCKMANN: Yes.

THE COURT: -- 3 being the average, as the company averages out, aggregates them to an aggregate of 3.2. Look, I appreciate that measured against a level of optimal, that's short, but measured against the company's statements, why is that indicative of inaccuracy?

MR. BRUCKMANN: Regarding the overall statement of

following NIST, your Honor?

THE COURT: Yes.

MR. BRUCKMANN: Your Honor, rather than getting into a metaphysical debate over what "follow" means, our core allegation on the follow NIST statement is that it's a materially misleading omission to claim to follow NIST without revealing how poor they score on certain critical components of it. In other words, it's a global that encompasses the other four specific allegations --

THE COURT: But even the global here gives them a maturity -- an aggregate level of just over 3, which, adjectively, puts it at solid, if you will — my word there, not theirs — but it's not an impeaching badly bad grade.

MR. BRUCKMANN: If that were the only issue. Follow NIST versus an overall grade, that might be a fair way to conclude, your Honor, but there are also specific conclusions regarding critical representations that were made on the website. And those are specifically misleading.

So even --

THE COURT: Give me your best examples of misleading statements from the security statement on the website.

MR. BRUCKMANN: Looking at Exhibit 5, Mr. Turner's declaration, on page 4 of 5, under "Access Controls," where it says "Role-Based Access" — forgive me. It's page 4 of 5 of the exhibit.

THE COURT: Got it.

MR. BRUCKMANN: Under "Access Controls, Role-Based Access," that entire first paragraph, including the specific representation that access controls to sensitive data in our database systems and environment are set on a need-to-know/least privilege necessary basis. That is specifically false as shown by, among other things, paragraph 194.

A few paragraphs down, "Secure Development Lifecycle." Again, that entire section is false, but among the specifics are the second sentence, "Security and security testing are implemented throughout the entire software development methodology." We have a number of allegations in the complaint regarding the lack of testing, including the fact that there was no penetration testing in December -- in 2018, as reflected in the December 2018 presentation.

Even if they did penetration testing later, that still means that this was false during the period of time where they were a publicly traded company. They can't get out of a 10b-5 allegation by making something true after it having been false for a period of time.

THE COURT: Although it might delimit the period of time covered by the claim.

MR. BRUCKMANN: It potentially could, it could go to something like penalties, but in terms of pleading liability,

if it's false in October of 2018, it is false.

THE COURT: May I ask you, just to the extent that access control seems to be the strongest of the deficiencies that you've pled, is there a link between that and what later happens with SUNBURST?

MR. BRUCKMANN: There absolutely is, your Honor. We don't say it's a but-for cause, but in paragraph 256 of the complaint, we specifically talk about how the threat actors exploited the lack of access controls in order to be able to move throughout the SolarWinds network.

THE COURT: And how is that known? Paragraph 256 doesn't -- what's the factual basis for the statement that the threat actors — Russia, I take it — exploited this particular security problem?

MR. BRUCKMANN: Those documents produced to the SEC by SolarWinds. I believe it was a presentation by the law firm DLA Piper. It was a series of PowerPoints that walked through how the attack had happened, and that's where it talked about that the first known access was in January of 2019, and it was through the VPN network using a former employee's credentials.

THE COURT: So stepping back, let's suppose, for argument's sake, that the statements in the security -- what's it called?

MR. BRUCKMANN: The security statement.

THE COURT: -- statement — thank you — were at some

point after the IPO regarded as misleading. Explain to me the theory of scienter here. To begin with, is the company's scienter here, as pled, solely derivative of Mr. Brown, or is there some other basis on which the SEC is contending that the company had the relevant scienter?

MR. BRUCKMANN: For the security statement, we're saying it's through Mr. Brown.

THE COURT: Not through some other human being, it's respondeat, in effect, through Mr. Brown?

MR. BRUCKMANN: Yes.

THE COURT: So what's the basis for Mr. Brown having scienter to defraud investors as opposed to arguably to overhype to customers?

MR. BRUCKMANN: Well, scienter is not a specific requirement that someone have an intent to deceive investors. I'm not aware of any case saying it has rise to that level. The SEC has two theories regarding scienter. We are not backing away from either of them.

The first is this was a deliberate scheme by Mr. Brown, starting well before the relative period, to affirmatively portray SolarWinds as a cybersecurity leader when they were, in fact, a cybersecurity laggard. And it began with the posting of the security statement, and included his podcasts, his presentations, press releases, and everything else that went into it.

The second is simply — and this is in *Novak* and other Second Circuit cases — that he knew or had access to information that the specific representations in the security statement were false, and that is pled throughout the brief, your Honor, throughout the complaint.

THE COURT: Although not necessary to plead it, not irrelevant is motive.

What's his motive?

MR. BRUCKMANN: The motive would be to have SolarWinds continue to obtain and retain business. And while that's not enough to be establishing scienter on its own, it is a motive that people can have.

THE COURT: So if that's not enough to get there on its own, what else do you cite as clearing the pleading bar for Mr. Brown's scienter? In other words, there's not, I think, a pleading about stock trading of consequence, there's no pleading about seeking promotion or something. I gather part of the theory is that he inherited a bad system as opposed to put it in place. What's the motive?

MR. BRUCKMANN: So what we plead for scienter would be, under *Novak*, that he knows information that contradicts the public statements. That is sufficient, without any motive whatsoever, to establish scienter under *Novak*.

THE COURT: Is there any allegation that he made false statements north of him in the food chain?

MR. BRUCKMANN: No, but there's information that is not reported up.

THE COURT: And what's the fair inference from that?

MR. BRUCKMANN: That he doesn't want to be seen as doing a bad job as the cybersecurity point person at the company.

THE COURT: All right.

What's the basis for Mr. Brown's -- assume, for argument's sake, just that the risk disclosure were actionable. What would be the basis for tying Mr. Brown to it, and for pleading his scienter? I should just ask, whose scienter is relevant to the risk disclosure statement? Who are you basing that on?

MR. BRUCKMANN: For that, we have two alternative theories. One is that it's Mr. Brown; and, two, that if it's not Mr. Brown, that it would be, under *Teamsters* and other cases, that essentially someone must have had scienter given how different that was than the reality on the ground. But our --

THE COURT: Let's focus on the Mr. Brown angle. What's the basis?

MR. BRUCKMANN: Courts in this district have repeatedly held that the person who makes a statement does not have to be the person who has scienter as long as there's connective tissue between the person who has scienter and the

statement.

We go through, in the amended complaint, that Mr. Brown was specifically consulted and asked questions and knew that that was information that was going to feed into the risk disclosure. He is the person in charge of cybersecurity at SolarWinds, and he certified, we believe incorrectly and falsely, on various subcertifications regarding the state of cybersecurity at SolarWinds that were used to reaffirm the risk disclosure --

THE COURT: So you are pleading that he, in effect, misleads people north of him as to the health of the cybersecurity environment?

MR. BRUCKMANN: Through the subcertifications, yes.

THE COURT: Where is that in the complaint? I may have missed that.

MR. BRUCKMANN: Court's indulgence?

THE COURT: Of course.

(Pause)

MR. BRUCKMANN: Yes, page 93, paragraph 298, your Honor.

THE COURT: One moment.

"Nonetheless, Brown signed subcertifications relied on by the senior executives" --

MR. BRUCKMANN: Yes, exactly.

THE COURT: -- "confirming that all discrepancies,

issues, or weaknesses had been disclosed to the executives responsible for the security filings." That's the money sentence?

MR. BRUCKMANN: Yes.

THE COURT: Okay.

MR. BRUCKMANN: And he had not reported up, among other things, the combined U.S. Government Agency A and Cybersecurity Firm B or the U.S. trustee problem and Palo Alto Networks, the two entities. He had not reported that up to the C-Suite.

THE COURT: So as to that, as to the -- the agency, what is it government agency A and company B?

MR. BRUCKMANN: Yes.

THE COURT: Based on the pleadings, does knowledge of that go north of Brown of those incidents at the time?

MR. BRUCKMANN: One of them is reported to the chief technology officer.

THE COURT: Who at the time was Brown's boss?

MR. BRUCKMANN: Brown's boss' boss, to be very precise.

THE COURT: Okay.

MR. BRUCKMANN: But no one above Brown is told about the combined two incidents. And it is the combined two incidents that really makes it material. The one thing I think that Mr. Berkowitz said that I agree with is that when figuring

out when something needs to be updated in the risk disclosure, the question is materiality. And after the U.S. Government Agency A attack, Brown assessed — essentially this is one of two things — either the hacker was already at U.S. Government Agency A when SolarWinds arrived on the scene or someone is looking to use Orion as part of a larger attack. And it was described as spooky and concerning within SolarWinds.

Once the second one happens, and numerous people within SolarWinds are linking and talking about how similar those are, essentially at that point, Brown either knew or was reckless in not knowing that of the two scenarios he outlined, it was the second one, that someone was looking to use Orion in the scheme of broader attacks.

THE COURT: As pled, what's the basis for the similarity? I thought it was not until C, that the company actually gets its eyeballs on the code itself?

MR. BRUCKMANN: So if your Honor looks at, I believe it's, paragraph 281 --

THE COURT: They say multiple employees -- you say recognize the similarities. One of them says seems similar, another says, "we have similar case."

That's about it. I mean, other people reference the other attack, but don't say similar. But beyond the fact that you've got that top-level use of the word "similar," is there any factual basis? For example, is there any pleading about

what these employees based that on collusion on?

MR. BRUCKMANN: Yes, your Honor. It talks about both using the business-layer host, which is a specific part of the Orion improvement program in order to conduct the attack. And if you continue into paragraphs 282 and 283, when having a phone call with company B, company B asked pointblank if SolarWinds had seen similar activity before. SolarWinds knew they had seen similar activity before and denied it. And that's what led to that instant message of the employee, "Well, I just lied."

THE COURT: Right. Is that something that Brown is accountable for?

MR. BRUCKMANN: It's people within his group. We don't have him directly tied to that, but those two people report to Brown.

THE COURT: Okay.

Same question, though: Is there a basis for Brown knowing that some underling of his, in effect, ducked the question of whether there was some prior incident?

MR. BRUCKMANN: We don't have Brown tied directly to that statement, no, your Honor.

THE COURT: Look, Mr. Berkowitz's argument about attacks A and B was that they weren't well tied together and they didn't ultimately impeach the risk disclosure, which describes this very thing.

I'd welcome if you want to examine the language of the risk disclosure. I understood you to be focusing on the distinction between potential and something else.

MR. BRUCKMANN: Yes.

THE COURT: I think we need to have the risk disclosure up. Let me ask defense counsel, just for --

MR. BRUCKMANN: We can do that.

THE COURT: -- for everyone's benefit, let's put the risk disclosure up.

Sorry, that's the risk disclosure. Yeah, that's right.

So what is actionable about the risk disclosure once Company B reports to SolarWinds?

MR. BRUCKMANN: The risk disclosure — and this is the way SolarWinds described it in their brief at page 4 — simply discloses that, like any technology company, SolarWinds is vulnerable to there being cyber attacks. It does not contain company-specific assessment about their individualized and heightened risk due to their poor cybersecurity framework overall and the specific incidents that they had seen in 2020, which include both the U.S. Government Agency A and Cybersecurity Firm B, but also, as we discuss in the amended complaint, the series of attacks on their MSP customers that indicated that there were potential reasons to think that someone had gotten inside of SolarWinds because of the way they

were able to attack the MSP customers.

THE COURT: What about the case law that Mr. Berkowitz cited on risk disclosures in particular?

MR. BRUCKMANN: Well, your Honor, I think the best case on risk disclosure specifically is the Second Circuit's decision in *Meyer*, where it says, "A generic warning of risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor's calculations of probability." SolarWinds did recite all of the things that could happen if they were hacked. We don't dispute that. They did not give any indication as to why it was more likely that they would be hacked compared to any company, which they should have, given the problems and red flags they had seen.

THE COURT: Did they have that obligation, in your view, after learning from just Government Agency A?

MR. BRUCKMANN: Well, we think they had an obligation from the moment of their IPO, based on the overall flawed cybersecurity posture, the lack of access controls, et cetera. But in terms of was there something specific triggered by the attacks, we're saying certainly after the second one and the linking, that that's when, regarding the attacks, there's an obligation.

THE COURT: Is there any evidence that Mr. Brown — who seems to be the principal basis of your pleading scienter, based on the risk disclosure — drew the connection between A

and B?

MR. BRUCKMANN: Well, he knew that the BusinessLayerHost was used in both. That's in paragraph 280. He had described the attack on U.S. Government Agency A as unique. So when you have an attack that you think is unique, that you're describing as, you know, one of two scenarios, and then you see another hack attack happening in a similar fashion, I mean, we don't need Brown to have said, "I put it together." The standard cannot be that someone has to actually type down in a document that they have linked two things, in order for it to be actionable conduct.

THE COURT: Do you have communications with Brown that analogize or link, even in somebody else's mind, A and B?

MR. BRUCKMANN: Court's indulgence.

(Pause)

MR. BRUCKMANN: In paragraph 280 there's the talk about the similarity of the use of the BusinessLayerHost in both attacks.

THE COURT: Is Brown on those communications?

MR. BRUCKMANN: Yes.

THE COURT: Yes, it says: An email later forwarded to him, a couple of days later, said that B -- it seems like they had a breach similar to A. This does not appear to be OIP, that we know of yet, related, but the BusinessLayer was used in the attack chain, according to them.

What does "OIP" mean?

MR. BRUCKMANN: That's the Orion Improvement Program. That is explained in an earlier part of the complaint.

THE COURT: I see.

"In this case, however, it was to do," and then it says, "[BusinessLayer] running some malicious download."

Is it clear from those sentences that Brown is being told that these two are related, or is it just --

MR. BRUCKMANN: Yes.

THE COURT: -- being theorized?

MR. BRUCKMANN: Well, the language of the email is "Cybersecurity Firm B in touch with customer support, and it seems they had a breach similar to U.S. Government Agency A."

THE COURT: Right. And then it says, "It doesn't appear to be Orion-related," suggesting that there's a breach but apparently not deriving from the Orion, meaning the SolarWinds software.

MR. BRUCKMANN: No. OIP is a specific part of Orion, the Orion Improvement Program. Earlier in the complaint it makes very clear that the Cybersecurity Firm B attack was definitively Orion.

THE COURT: All right.

I guess I'm trying to decode a not completely lucid email chain from an anonymous employee that is forwarded to Brown, and trying to understand the extent to which it should

put him on notice that these are very likely deriving from the same actor as opposed to bearing some similarity.

MR. BRUCKMANN: Both are definitively Orion. Brown describes U.S. Government Agency A, around the time it happens, as unique, as very concerning, and of one of two things, either someone is already there or they are looking to use Orion in part of a broader attack.

Then he gets an email saying that B, also Orion, is similar. He knows that BusinessLayerHost is again involved.

And the only sort of contraindication, I guess, is that the specific subpart of Orion, the Orion Improvement Program, according to this email, was not necessarily involved in the second one.

THE COURT: So what, from your perspective, after B, should -- if Brown was responsible for getting the company to adjust its risk disclosure, at this point there's, from your perspective, circumstantial evidence, but not dispositive evidence. What's the change that is required to be made to the risk disclosure, from your perspective, at that point, to bring it into compliance?

MR. BRUCKMANN: Well, Brown's specific responsibility would have been to report it to the disclosure committee, to the C-Suite, that he had concluded that there was a potential similarity between two attacks.

THE COURT: Right. But that's not what the claim is

against Brown.

MR. BRUCKMANN: Right.

THE COURT: That may have been an employment misstep by him, but it's not a basis for liability. I appreciate that you've got a disclosure controls question, and Brown's nondisclosure of that may be probative, or not, on that.

But my question to you is: What's the correction to the risk disclosure that's needed to make it not, from your perspective, misleading after the company knows about B?

MR. BRUCKMANN: After the company knows about B, it also already knows about the series of attacks on the MSP customers, and it knows about issues like its access controls. It had some obligation to update the risk disclosure to indicate something about the increased probability of an attack at SolarWinds as compared to a generic technology company.

That's what *Meyer* talks about --

THE COURT: Without binding yourself to specific language, give me an example of language that would have captured the somewhat uncertain state that the company was in at that point.

MR. BRUCKMANN: I mean, it's not the SEC's job to write disclosures for companies, but --

THE COURT: But if the SEC can't come up with language that would be up to the task, it raises a question of what whether this is a viable theory.

I welcome, just broadly — what do you have in mind here? "We disclose that we are presently investigating the presence of malicious software on two customers of our Orion product"? Is that essentially what you have in mind?

MR. BRUCKMANN: Something along that, or "We've seen indications that someone is looking to use Orion in a broader attack," which was Brown's essential conclusion in the first email. It's one of two things. But, by B, it's pretty obvious which of the two it is.

THE COURT: Okay. In effect, what you're saying is that the allegation really needed to capture the newsflash that there had been two seemingly similar attacks through Orion?

MR. BRUCKMANN: Yes.

THE COURT: What did the company know from the two customers, as of the time of the two disclosures? What did they understand, as reported by the customers, to have happened, according to the pleadings?

MR. BRUCKMANN: So, for U.S. Government Agency A, that they were doing a test run of Orion, and then when doing that test run, they saw it reach out to an apparently malicious server.

THE COURT: Okay. And B?

MR. BRUCKMANN: B reported it to SolarWinds as being part of what they called a red-team exercise. That ends up not being truthful, frankly. Cybersecurity Firm B was being

cautious in terms of what they revealed about their own cybersecurity problems to SolarWinds.

THE COURT: Well, truthful or not, what did SolarWinds understand at the time?

MR. BRUCKMANN: I want to make sure I get this correct, your Honor. That it was, again, the Orion server reaching out --

THE COURT: To a malicious server?

MR. BRUCKMANN: I believe that's the case, your Honor, but I want to make sure I get it correctly.

So it's paragraph 279. And, yes, it was described as malicious activity by the Orion software, including the BusinessLayerHost reaching out to a website and downloading a malicious file.

THE COURT: So the BusinessLayerHost reaching out to a malicious website is the connective tissue between A and B, as known to SolarWinds after B? Is that a fair synopsis of the similarity?

MR. BRUCKMANN: To be super precise with the language of the amended complaint, Cybersecurity Firm B isn't described as describing it as a malicious website; it was reaching out to a website and downloading a malicious file. But reaching out to a website with malicious activity, I think, is the connective tissue between the two.

THE COURT: Come back, then, just to the issue of

scienter as to that.

If the information flow stops effectively with Brown at that point, putting aside whether he should have done his job better, what's the scienter point here with respect to him and the risk disclosure? I take it he has no authorship of the risk disclosure, and, on the pleadings, I don't think it's ever really run by him for review.

I completely get the theory of scienter with him as to the security statement, but as to the risk disclosure?

MR. BRUCKMANN: He is the person with the knowledge of the events, who is supposed to report it up, according to the company's disclosure policy, which requires incidents that could impact -- or for which multiple customers are susceptible, to be reported up, and he doesn't. And by failing to do that, the information is unable by the company to be assessed and reported out.

THE COURT: Sure. Why isn't the other word for that is that he was negligent?

MR. BRUCKMANN: Because he had actual knowledge of the information regarding Cybersecurity Firm B and Government Agency A.

THE COURT: And he booted a job requirement. But that's a little different from securities fraud scienter?

MR. BRUCKMANN: Well, we go back to the same subcerts then, your Honor, we discussed previously, that he is signing,

saying all information has been reported up when, with regard to --

THE COURT: Does he do that after B? Is the allegation that at some point after B he falsely signs a relevant certification?

MR. BRUCKMANN: My memory is that the subcertifications are quarterly. I'm trying to remember if that is in the amended complaint or not.

I think it's a fair implication, looking at 298 and 299, because 299 talks about the quarterly reports that are done based on the subcertifications.

THE COURT: All right. You had mentioned that there was an alternative theory of scienter with respect to the risk disclosure that is not Brown.

What is that theory?

MR. BRUCKMANN: Under the *Teamsters* case and other cases, at the pleading stage, the plaintiff does not have to identify whose specific scienter is imputing to the company where the statements are so divorced from reality that somebody must have had scienter.

THE COURT: And at what point then -- is it summary judgment at which you would be accountable to that --

MR. BRUCKMANN: Yes.

THE COURT: -- the *respondeat* theory?

MR. BRUCKMANN: Yes.

THE COURT: All right.

I want to make sure you have enough time to address the back end here, involving SUNBURST. I don't know if that is you or Mr. Ney who's doing that.

MR. BRUCKMANN: The 8-K issue would be me as well, your Honor.

THE COURT: Go ahead.

And maybe I'll ask defense counsel, just because it does facilitate the discussion, if you don't mind putting up the relevant 8-K. Is the December 14 one?

MR. TURNER: Certainly, your Honor.

THE COURT: Thank you. I appreciate it.

All right. This disclosure is pretty bad news, and it drops the stock, apparently, by 25 percent, allowing for other market activity.

Is the problem with the word "potentially"?

MR. BRUCKMANN: That's one of the problems. There are several portions of this that indicate, essentially, it's unknown whether this has been successfully exploited or not. But there were clear conclusions by Brown and others that it had been successfully exploited by that point.

Defense points to the word "infiltration," but I want to point to some language that was used by Brown at the time.

Court's indulgence.

THE COURT: Of course. Just give me the cites to the

complaint.

MR. BRUCKMANN: Of course. That's what I'm looking for, your Honor.

So paragraph 315, your Honor.

THE COURT: Go ahead.

MR. BRUCKMANN: So, before that 8-K, internally, SolarWinds had concluded that the U.S. Government Agency A attack was a "customer compromise" and an "attack that was successful," and knew that the Cybersecurity Firm B attack was considered "a breach."

So quibbling over the precise definition of "infiltration" isn't the point. The point is, if that's the conclusion inside SolarWinds, it's at least a material omission to say "it could potentially allow an attacker to compromise the server" without disclosing that this is what had already happened.

THE COURT: Well, sorry. It's a customer compromise insofar as the Orion product has been corrupted in that way, but that's being disclosed, the vulnerability is inserted. Why doesn't that itself explain the words "customer compromise"? In other words, why does "customer compromise" mean that something beyond what's being disclosed here, which is the vulnerability inserted into the customer-bought product, qualify?

MR. BRUCKMANN: Well, then focus on the next one, your

Honor, "attack that was successful."

THE COURT: Right.

MR. BRUCKMANN: There's nothing about this 8-K that conveys that there had been attack that was successful --

THE COURT: What is meant by an attack that had been successful? What has Government Agency A told SolarWinds at this point beyond the fact that it has discovered this vulnerability in the Orion product?

MR. BRUCKMANN: That it's reaching out and contacting a malicious server.

THE COURT: What does "successful" mean? Just that the server was contacted, or that some follow-on damage was done? It's not a very specific term.

MR. BRUCKMANN: The case law makes clear that what's at issue here is not the literal truth of any word but whether, as a whole, this statement accurately conveys information to investors. There had been two attacks over a period of six months that were actively exploiting this vulnerability. And to say that simply it's potential and we're investigating whether it has been used, when they knew that twice it had actively been used --

THE COURT: But, sorry, the "potential" modifies something, "potentially allow an attacker to compromise the server." I thought what you were saying is SolarWinds knew, at the time of December 14th, that in fact the attacker had

compromised a customer server.

Is that what you're saying?

MR. BRUCKMANN: It depends what you mean by compromised a server potentially, your Honor, and that's probably a factual dispute.

THE COURT: No. It's maybe a pleading problem. I mean, that's the point here.

I appreciate that there are lots of different ways this could be written, but if you're trying to claim scienter, if you're not prepared to tell me that an attacker has, in fact, compromised the server on which the Orion products run, if you're not citing a factual basis to contend that Brown or SolarWinds knew that, what's wrong with the word "potentially"?

MR. BRUCKMANN: Well, look at the last bullet point on the screen, your Honor.

The last sentence of that is, "SolarWinds is still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks."

They know that successfully Orion is reporting out to malicious servers, they know that successfully Orion is downloading malicious code onto Cybersecurity Firm B --

THE COURT: But they are stating unequivocally in the first sentence that, in point of fact, the vulnerability has been inserted into a product that has been bought by customers.

MR. BRUCKMANN: Right.

THE COURT: So what does it mean for it to be thereafter successful? Does it mean that some degree of follow-on damages have been done to the customer? Does it mean that certain customer information has been liberated from the customer and sent back to the Russians? The problem with "successfully" is that it's a somewhat hazy term, so I am having a little bit of difficulty finding the term "successfully exploited" to be awful clear. It's not a term of art.

Putting the first and last bullet points together, the implication is that "successfully exploited" means some follow-on damage beyond the vulnerability being put in the customer product.

MR. BRUCKMANN: At Cybersecurity Firm B, it reaches out to the website and downloads a malicious file onto the Cybersecurity Firm B computer server. That is not just potentially. That is an actual act that shows this was being exploited.

Now, whether it's an infiltration or not, that is information that is materially different than what is conveyed here.

THE COURT: In other words, you're contending that the act of downloading necessarily means a compromise?

MR. BRUCKMANN: And it shows a --

THE COURT: Is that what makes bullet point 1 misleading?

MR. BRUCKMANN: Yes. I think to have malicious software downloaded onto a server is a compromise.

THE COURT: May I ask you — look, it's not lost on me that this has got to be a corporate crisis of the first order and within 48 hours, if not less, they pumped this thing out, which is pretty dramatic.

Does the case law give any allowance for the fast pace of events?

MR. BRUCKMANN: I think that's one fact that could be taken into account when looking at scienter, but what we have here is clear testimony from Brown that he essentially had instantly linked to all of these things together. So while we might have a very difficult factual time in some cases establishing that by the time of the disclosure, 48 hours later, someone had put it all together, he testified that he had.

THE COURT: Well, look, that suggests perhaps a different theory, on your part, which is that the fundamental problem with this disclosure is that it suggests there's just one, rather than three, cyber attacks.

Is that part of your theory of what's misleading?

MR. BRUCKMANN: Yes. The number is clearly part of what we allege is incorrect, as well as the length of time it's

been going on.

THE COURT: Because essentially bullet points 1 and 2 are phrased in the singular, a cyber attack, and this incident, as opposed to what somebody might take away as being more serious, which is three in some reasonably rapid succession?

MR. BRUCKMANN: Well, it was actually over a period of six months, which I think makes it even worse, your Honor, the fact that this had been out there and, you know, contacting, reaching out, for six months. This isn't just stray code that could be a problem. This is stray code that is actively acting up and downloading, in one instance, malicious code.

THE COURT: If this disclosure had been made after B, and instead of saying "a cyber attack," just to clean it up, said "two," would you have any problem with it?

MR. BRUCKMANN: The devil is in the detail, but if there had been some disclosure along these lines after B, I think that would have largely solved the specific problem with regard to the A and B attacks.

THE COURT: Okay. So what makes C worse is -- what more is known about C than about B and A? It's that it breached the server? It's that it was downloaded?

MR. BRUCKMANN: No, the download is B.

THE COURT: Okay. If this would have been basically adequate, subject to wordsmithing for B, what is it about C that makes this now problematic, inadequate?

You've just said to me, in substance --

MR. BRUCKMANN: Yeah, I regret --

THE COURT: You may regret it, but you've just said this language essentially would have more or less done the trick, if issued after B and referred to two and not one.

So what is it that's new that's learned about C that makes this language, put aside the number of cyber attacks, actionable?

MR. BRUCKMANN: I spoke too quickly when I said I would do it for A and B. So this does not convey that it had been actively exploited and the length of time when it had been actively exploited. That is the critical missing information.

THE COURT: Do you have any example of a case where a company is, in effect, responding to some exigency like this and a court has sustained as viable a disclosure as being inadequately fulsome?

MR. BRUCKMANN: None comes to mind, but that goes to scienter, not to falsity. If it's false, it's false.

THE COURT: Well, it's not false. It may be misleading, but it's not false.

MR. BRUCKMANN: If it's misleading, it's misleading. The rapid timing could go to scienter as a matter of evidentiary proof.

THE COURT: Who is the scienter based on, to the extent you're relying on the December 14th 8-K?

MR. BRUCKMANN: Brown.

THE COURT: And what's Brown's connection in the development of the 8-K?

MR. BRUCKMANN: He's in the room when it is being drafted and tasked with ensuring that it is technically and factually accurate.

THE COURT: All right.

And your point is that Brown, in effect, should have said, this is literally accurate but incomplete because it doesn't get to the full extent of the problem?

MR. BRUCKMANN: He should have said something about the A and B attacks and said nothing about the A and B attacks.

THE COURT: I've got a few more minutes for you because I've taken you perhaps off track. Continue on with the argument. I want to make sure you and your team cover what you need to cover.

MR. BRUCKMANN: I just want to check on time here. I do want to allow some time for the internal accounting controls piece of the argument as well, your Honor.

THE COURT: Okay. Just one moment.

(Pause)

THE COURT: Let's go ahead and move to that.

MR. NEY: Thank you, your Honor.

Your Honor, Brad Ney for the Securities and Exchange Commission.

Your Honor, following briefing, the parties are left with a very narrow disagreement on the internal accounting controls issue, and a brief example will make this abundantly clear:

Your Honor, I previously worked in the restaurant industry and the restaurant storeroom. And that storeroom had a padlock on it, and two managers had the key to that padlock. And that was the storeroom that kept all of the liquor for that restaurant.

In order for an --

THE COURT: The statute of limitations has run on the war story you're about to tell me?

MR. NEY: Your Honor, it was an effective internal control — that's what I can tell you — and an internal accounting control.

In order to get access to that room, in order to get stock for the bar, you had to go to one of those two managers; that manager had to use their key to open the padlock so that they could be present as you took what was in that room out of the room. Your Honor, that padlock was an internal accounting control, in that context.

Now, if your Honor held up a padlock and said to me, counselor, is this an internal accounting control, the answer would be, it depends what you use it for, your Honor. The same with the two managers. The fact that only two managers had a

key to that storeroom was also an internal accounting control.

Again, your Honor, if you held up a key --

THE COURT: That's because a valuable asset could get stolen?

MR. NEY: That's correct. That's because there was a valuable asset in that room.

Your Honor, if the padlock is used as part of a plan or procedure to restrict unauthorized access to the corporation's assets, then it's an internal accounting control. That's why I said this is a very narrow issue for your Honor. The only question is whether or not SolarWinds' source code, its Orion product code, its customer databases, and its IT network were assets. And, your Honor, the answer is simple, and the answer is yes.

THE COURT: So any company that's got holes in its computer infrastructure, in that case — if materially bad things could happen to the company, if that hole is exploited — is liable under this theory?

MR. NEY: If an actor could get access to the assets of the company through that website. For example, your Honor, if this was a paint company and the paint company had a website that was out there for purposes of advertising to people — here are the different colors of our paint — but you couldn't get access to the company's assets through that website, then the controls against malicious activity on that website would not

be an internal accounting control.

THE COURT: Sorry. I was struck, from the briefs, by the absence, I think, of any case that articulates the theory you're articulating.

Do you have a case that says something like this?

MR. NEY: Your Honor, I would say the *World-Wide Coin* case actually makes this abundantly clear in the physical space. So, in *World-Wide Coin*, it was a coin company, they had bags of valuable coins that were left in hallways and in unlocked conference rooms, they had a vault that was left open that every employee had access to. And the Court found that the company had ineffective internal --

THE COURT: Somebody could walk off with them depriving the company of that?

MR. NEY: They could --

THE COURT: What's depriving SolarWinds of its software just because its software may be a bum product? In other words, if you're the customer you're pretty disappointed, and maybe you want your money back, but why does that make it an accounting control?

MR. NEY: It's an accounting control, your Honor, because SolarWinds software code and because its Orion product are assets. They are not just assets in the colloquial sense, like the Chamber of Commerce says; these are assets in the accounting sense. They show up on SolarWinds' financial

statements. They're intangible assets. They're described as developed product technology --

THE COURT: Sorry, SolarWinds still has its software code. What it has sold to its customer has been compromised, but back at the shop they've got their software code.

Again, the customer could be plenty peeved, but I'm having difficulty understanding why they have lost this asset as opposed to sold a bum product to a customer.

MR. NEY: Your Honor, this goes to the argument that counsel made in their reply brief, which is that somehow intangible assets are not subject to loss. You can't have a loss of intangible asset — I think counsel said — because it doesn't vanish when someone steals it.

Your Honor, it's totally inconsistent with the legal definition of "loss." So, your Honor --

THE COURT: Wait a minute, wait a minute.

Upon learning about this, presumably, SolarWinds gets some techie who solves the problem and then it's got its software again in shipshape.

What asset has it lost? It's treated a customer shabbily, but ultimately it is able to presumably restore the problem by basically debugging the system.

MR. NEY: Your Honor, let me give an example.

If a person was to walk up to the Mona Lisa, slash it with a knife, that could be fixed, but the fact that a person

went up and slashed that with a knife caused a loss at the moment that happened. And whoever owns that painting is going to have to spend a lot of money in order to fix that painting. The money it takes to fix that painting, the money it takes to fix this software code, is a loss to the company.

THE COURT: Is there any pleading as to how much money it cost the firm to repair the software code to get the bug out?

MR. NEY: That is not pled in the complaint, your Honor.

THE COURT: Is there any pleading that that is material as -- just the corrective? Is it on the pleadings? Could it have taken some smart person a day just to clean up the bug?

MR. NEY: So, your Honor, there is not a materiality requirement with respect to Section 13(b)(2)(B) in the first instance. If an individual is able to get access to the company's assets and do malicious things with the company's access, that is a problem under Section 13(b)(2)(B).

Your Honor --

THE COURT: There's no pleading here of the downstream damage from customers wanting their money back. That was a silent part of the complaint, that the customers who are buying a product that turns out to be corrupted -- there's no allegation here about what that cost the company to make things

right with the customers.

MR. NEY: There is not, your Honor. We do know that the Orion product accounted for 45 percent of the company's revenue. We know that it took money for the company to fix that, but --

THE COURT: There's no pleading?

MR. NEY: There's no pleading on that, your Honor, that is correct.

Your Honor, I will give another example, and I think this speaks to it: I would just suggest that it would be an astonishing outcome to say that intangible assets, because they don't vanish when they are stolen, somehow are not an asset or not an asset subject to loss.

THE COURT: The defendant says the astonishing outcome would be to call what happened here an accounting control violation as opposed to some other, like, cybersecurity control violation.

MR. NEY: Well, your Honor, again, the reason it's an accounting control violation is because they were assets of the company, and they were valued as such. If SolarWinds had been trying to sell its assets at the time that its software was compromised and another party realized that software was compromised, that software would be worth far less than what it stated it was worth. That is the difference.

At the time the software was compromised — and we know

now this was for a long period of time, it was for many months, at the least — during that period of time, that software was worth less than what SolarWinds claims it was worth.

Your Honor, if someone stole Coke's secret formula, the fact that Coke still has that formula written down does not change the fact that they've lost that information --

THE COURT: Well, it's because Coke then has a competitor. That's not what's alleged here.

Mr. Ney, you're over the SEC time. I need to give the other side its opportunity to rebut, but thank you.

MR. NEY: Thank you, your Honor.

THE COURT: Mr. Turner, just before we get to that, this may be on Mr. Berkowitz's side of the house, but just a brief response on where we just were on accounting controls.

MR. TURNER: Accounting controls, your Honor, it all comes down to bean counting. It's about securing the beans so they can be counted. So it's about tangible inventory assets. Yes, it's tangible assets. Nobody stole the software here. Vulnerability was inserted in the software. That's something bad that happened to the software; it's not a loss of the software.

THE COURT: But Mr. Ney's argument is that there's no materiality dimension, and so whatever damage needed to be corrected, at some cost, reflected at least a temporary diminution or a cost item for the company.

MR. TURNER: This has nothing to do with what that provision is about. That provision is about making sure that assets — tangible, countable assets — can be secured so they can be accurately counted. This is not an asset that can be counted, in the first place. If we're talking about boxes of software on a shelf, that's one thing, but this is just the code. So I'll let our brief speak for itself.

THE COURT: Very good.

MR. TURNER: Your Honor, there's been so much discussion about the DOJ and the PAN attacks and when they should have been disclosed. I think there's been a lot of confusion, including from the SEC, about what this case is ultimately about. When they brought this case, at the initial conference, they said this case is different from previous SEC cases, where there was a cybersecurity incident that wasn't necessarily disclosed in a timely fashion. Once SolarWinds became aware of a breach, they quickly made a disclosure.

This is not a case about a company that knew a material attack had occurred and failed to disclose it. The company would only have an obligation to disclose a cybersecurity incident if they had determined they had suffered one and that it was material.

THE COURT: Sorry, but, if I may, the SEC says that there was connective tissue between A and B that its pleadings sufficiently allege.

MR. TURNER: Let me just back up, your Honor, because these incidents that we keep talking about, these were not customers reporting that they had discovered malware in Orion. That's not what's even alleged. They allege suspicious activity. The Orion server is contacting some unknown website. What is that?

So the company is trying to figure out what it is, but they never determine the root cause. This is the SEC looking back in hindsight and making it sound easy.

THE COURT: So you have several employees who, at least according to the complaint, are drawing out the similarity, apparently, to Brown.

MR. TURNER: Similarities and differences, your Honor.

So you looked at a statement earlier that said, "This does not appear to be OIP," the Orion Improvement Program. The Orion Improvement Program was involved in DOJ. So that statement was basically saying this PAN incident does not look like it involves OIP. That was a difference.

THE COURT: How do we know OIP was involved in DOJ?

MR. TURNER: That's part of what's alleged, and that's true.

THE COURT: Okay.

MR. TURNER: So the point is, there are some similarities here but there is no conclusion drawn. The company is trying to figure it out. They're looking at --

trying to find vulnerabilities in their own software to explain what's happening. They can't find it. And part of this, your Honor, is that the mere fact that a server looks like it's contacting a website doesn't necessarily mean there is a problem with the software, in the first place. It could be the attacker disguising their activity to look like it's coming from SolarWinds when it's actually not. There are lots of things going on here that the company has to figure out.

The bottom line is, they allege in their complaint repeatedly, SolarWinds never was able to determine the root cause. That means they don't know what happened. They don't know that there's malware in their system. They don't know that a breach of SolarWinds is the root cause. That means there's no material incident to report.

THE COURT: Come back to the December 2014 8-K.

Putting aside the "potentially," the argument based on that word, it is notable that they describe this as a cyber attack. But, as of this point, hadn't the company drawn some connection between the Victim C cyber attack and Victims A and B?

MR. TURNER: This is, again, the problem with ambiguities of language. As your Honor was getting at earlier, what Brown was able to figure out, according to the complaint, is, he was able to link the suspicious activity that he had seen before to this malware that this third customer had

informed him about. So all that he's concluded is that DOJ and PAN had the malware on their system.

And I would add, your Honor, they justly conceded something that they did not allege in their complaint, they didn't disclose in their complaint. PAN described what happened to them as a red-team exercise, in other words, a simulation that they were doing. They didn't even disclose that it was an actual attack on them.

THE COURT: In other words, we have to take as true what was known to --

MR. TURNER: Yes.

THE COURT: -- SolarWinds, and what was described to SolarWinds, to some degree, minimized the facts that might have enabled it to draw a better connection?

MR. TURNER: They never allege that Mr. Brown or anybody else at SolarWinds concluded there has been an attack on SolarWinds and that's what explains these two incidents. Never. What they do is, they say "knew or should have known." This is SEC hindsight, looking back, and saying "should have known," but there's no allegation that anyone actually knew it.

THE COURT: The question I asked SEC counsel involving quick responses by corporations to crises like that — is there a line of cases that evaluates the latitude a company has in trying to get something out in a very short period of time?

MR. TURNER: It's a Seventh Circuit case, your Honor,

that we cite in the brief — *Higginbotham* I believe it is — that we cite in our brief. And it basically explains what your Honor is getting at, that the company here said it was still investigating. It was still investigating whether this downloaded software, that up to 18,000 had downloaded — that's what it was disclosing here — it was still investigating whether the attacker had used that successfully to infiltrate the network.

Again, if you look at this diagram, what Brown allegedly linked to the DOJ and PAN incidents was the malware. So he knows, allegedly, that the malware was on DOJ and PAN systems. The malware, by design, beacons back. That's the malware acting. That was what it was coded to do.

In terms of successfully exploiting that back door, it takes more than that. The attacker then has to see the malware beacon back and say, hey, I've got a server I can infiltrate, go through that server and get to the rest of the network --

THE COURT: That just gets to what the meaning is of "successfully exploits."

MR. TURNER: It has to mean that --

THE COURT: What's the "that"?

MR. TURNER: "Exploit" here has to mean something more than just having the malware downloaded in your system. The company had disclosed that up to 18,000 customers had the malware downloaded on their system.

So when they're saying they're investigating whether it was successfully exploited, they're not talking about whether it was successfully downloaded. They're talking about whether it was successfully used by the attacker --

THE COURT: What might exploitation or use be? What would be the next bad step?

MR. TURNER: It's 6 and 7 on this diagram. This is a judicially noticeable report from the U.S. Government. So, once the malicious code beacons out of a threat actor, then the threat actor can try to use the back door to get into the rest of the system, the rest of the network. That's where the valuable information is. The attacker doesn't care what's in the Orion server. That's not where the customer's valuable information is. They're trying to use the Orion server as a doorway into the rest of the network.

They never allege that DOJ or PAN ever told SolarWinds that it happened to them or the third customer.

THE COURT: Got it, all right.

MR. TURNER: What does this matter anyway? The disclosure essentially disclosed that the Russians had a back door in up to 18,000 customers. Who cares whether two of those customers were known specifically to SolarWinds?

THE COURT: In other words, that's the response to the singular versus the plural?

MR. TURNER: That's the response generally to the

fixation that the SEC has on the DOJ and PAN incidents, because there are two out of up to 18,000, and that's where the market reacted to, is up to 18,000. That is the outer universe of liability here. That's what an investor would be concerned about.

On scienter, your Honor: There's just a couple of things I want to get to there.

In terms of scienter, as to the risk disclosure, the key point is that if they're trying to impute Mr. Brown's scienter, the scienter has to be knowledge that that statement, that the risk disclosure statement, is false. He couldn't even have that knowledge if he never even saw the statement to begin with.

THE COURT: Sorry, what's the basis that he never saw it, as opposed to he didn't author it?

MR. TURNER: Paragraph 242, your Honor. But, generally, they never allege that he saw it, reviewed it, approved it. They only vaguely allege he gave some information that may have been used as part of it, but that's not enough on its face, and they don't --

THE COURT: I take it he was deposed and so, had he admitted seeing it, that was available to be cited?

MR. TURNER: He was deposed, your Honor.

In terms of like intentionally hiding or -- excuse me, not intentionally, but not passing up information to officials,

officers north of them, first of all, it's not even a negligence issue; it could be a disclosure controls issue potentially.

But in terms of not reporting stuff, most of their allegations about the supposed weaknesses in SolarWinds' security controls are from presentations Mr. Brown made to management. They repeatedly cite the quarterly risk reviews. That is Mr. Brown apprising on a quarterly basis the people above him about cybersecurity risks.

In terms of the subcerts they point to, those subcerts were for internal controls over financial reporting, SOX systems specifically. The Chamber of Commerce brief notes that the company's auditor found no material deficiency with respect to those controls.

So it's just a nonissue. And the risk disclosure was not about internal controls over financial reporting. The subcerts are just a complete red herring here.

THE COURT: What about the SEC's argument that on the pleadings it can allege scienter without pegging it to a particular actor within the company?

MR. TURNER: They're trying to draw on the collective scienter doctrine. We explain this in our brief, your Honor. That only applies where the misstatement is so dramatic that you have to assume that somebody knew -- like, for example, if a company had asserted that it had sold a million vehicles or

manufactured a million vehicles and it actually had manufactured zero. Here, we're talking about the risk disclosure, which says the company was vulnerable, which was true.

I mean, to say that that is so dramatically inaccurate --

THE COURT: In other words, there's a *res ipsa* quality. If the statement is blindingly false, it's reasonable to infer that there's a person with knowledge, but if it is --

MR. TURNER: Blindingly true.

THE COURT: -- or arguable, arguably imprecise and with a different colorations that the parties have, you're saying, even taking the SEC's characterization, it doesn't have that same *res ipsa* quality?

MR. TURNER: I don't even know what the characterization is. Your Honor, you asked him repeatedly, on several occasions, what language should the company have used. And they paused and they said, well, it's not our job. That is the whole problem here. Again and again, they can't articulate any principle for their position.

That's why you have amici who have filed the briefs in these cases — because if the SEC's position stands, then public companies across the spectrum are going to be left guessing, what do we have to disclose? If Microsoft has some customer incident, which they get hundreds of times a month, where it

receives suspicious activity, does that mean that we now have to run and file an 8-K or update our risk disclosure? What does this mean? They can't articulate it. That is why these theories should be dismissed.

THE COURT: Thank you, Mr. Turner.

Before we adjourn, I want to again thank all counsel for not just very effective briefs but a very effective and illuminating argument. I'll take the case under advisement.

I want to also, as well, say what I didn't say before, which is, to the extent there are representatives of the amici here, thank you, as well, for participating in the way you did. That added a lot of value, and I appreciate it.

We stand adjourned.

(Adjourned)